The application of Mobile-Commerce in the University and Its Security Concerns - a case study of Coventry University

Tripathi, R., Dai, Y., & Fei, X.

Proceedings of the 15th International Conference on Automation & Computing, University of Bedfordshire, Luton, UK, 19 September 2009

The application of Mobile-Commerce in the University and its security concerns – a case study of Coventry University

Raghvendra Tripathi, Dr Yang Dai*, Dr. Xiang Fei
R. Tripathi, MBA student, EKM, Coventry University, UK
Dr. Y. Dai: Senior Lecturer, EKM, Coventry University, UK
Dr. X. Fei, Research Fellow, CDE, Coventry University, UK
*Contact email: y.dai@coventry.ac.uk

Abstract*—The term M-Commerce (Mobile Commerce) is all about data capable mobile devices which are currently in use around the world by millions of users and enabling them to carry out financial transactions from anywhere at any time. However, security mechanisms still remain unexplored. As security plays a crucial role in facilitating the level of trust and confidence of users in mobile devices and applications, for better adoption of M-Commerce, satisfactory levels of trust have to be established in the underlying security of mobile devices and applications. This paper discusses the University M-Commerce application and its security issues. A survey and interviews have been conducted to obtain the consumer and supplier's perspectives. In addition, different types of mobile security technologies leading to better security levels have been described and analyzed for organisations, within the context of conducting mobile commerce via mobile networks. The conclusion shows that most of the students are ready for the campus M-Commerce, and the University can start the M-Commerce by providing the services that students prefer but with lower security requests.

Keywords - M-Commerce; Campus M-Commerce; M-Commerce security; Mobile Security.

1 Introduction

M-Commerce is viewed as the next generation of E-Commerce (Liang et al. 2007), which is based on the wireless telecommunication networking technologies, and mobile handheld devices, in order to exchange, buy or sell commodities, services or information (Kao et al 2003, Lee et al 2004, Elliott, 2004, Wei et al 2009). Barnes (2007) identifies the unique differences of M-Commerce from E-Commerce as reachability, accessibility, localisation, identification and portability. The drivers of Mobile-Commerce, due to the advantages of mobiles, are throughput time, portability, accessibility, flexibility, mobility, efficiency and convenience (Segev 2003, Chen and Skelton 2005, Deibert and Rothlauf 2006, Khalifa and Shen 2008).

In 2001, the total revenue of mobile services was less than nine million in the whole of Western Europe (Tiwari et al 2008). However, according to Portio Research, the total revenue generated by Mobile messaging was USD130 billion worldwide in 2008, and the value will be nearly doubled to USD224 billion by 2013. There are over half of the world population using mobile phones and the number will reach to 5.8 billion people, which equals to 80% of the world population by the end of 2013 (Portio Research, Mobile Marketing Magazine, Sept. 25, 2008). Yankee Group has predicted that mobile ad sales could reach nearly 1% of US ad sales, which is about $2 billions in total by 2010, and up to $10 billions by 2015 (Davidson 2006).

2 M-Commerce application and its implementation in the University

Hu et al (2004) state that M-Commerce can be applied in Commerce, Education, Entertainment, Healthcare, Transportation, Logistics, and Inventory fields. Sponge's study reveals that retail industry has higher M-Commerce usage, and 70% of 10 prominent online retailers use mobile to communicate with their customers, which cover various sectors such as travel, leisure, fashion, catalogues, communications and publishing (Sponge, see Mobile Marketing Magazine, Nov. 13, 2008).

Tiwari et al. (2008) classify the M-Commerce business into various types respectively: Mobile banking, Mobile entertainment, Mobile information services, Mobile marketing, Mobile shopping, Mobile ticketing, and Telematics services.

Although M-Commerce has huge potential market and business benefits, it always follows by the concerns about the privacy and safety of personal data, and its misuses (Tiwari et al. 2008). Taniar (2008) illustrates the main obstacles for the end users' adoption of M-Commerce as lack of security, consumer faith, non-universal standards and costs, device & usability issues, a shorter product life-cycle, and no appropriate business model. Thanh (2008) categorizes the M-commerce security into four types: authentication, integrity, confidentiality and non-repudiation.

3. THE M-COMMERCE IMPLEMENTATION IN THE UNIVERSITY

Davidson (2006) states that big brands, such as Pepsi and Nike, use Mobile phones and wireless devices as the hottest frontier to reach 18-34-year-old set (also see Armstrong and Kotler, 2009), since they are the dominant mobile phone users who might be the main M-Commerce market.

Universities have the largest 18-34-year-old population, and should have been pioneers of M-commerce implementation. However, only few universities in the UK have adopted M-Commerce in their campus. This research aims to find out why UK universities are reluctant to adopt M-Commerce and identify the obstacles of M-Commerce applications in the UK universities.

Coventry University had considered using M-Commerce to increase the quality of service in 2008, but later this plan was stopped due to the security concerns. This research uses Coventry University as a case study to trace the obstacles of the M-Commerce implementation in the University and the M-Commerce security issues involved in it.

VeriSign (2007) proposes four main components of M-commerce: Mobile operator, consumers, financial institutions, merchants and suppliers. Hence, this research has been designed to investigate from the above M-Commerce components, but the financial institutions have been ignored from this paper due to the unavailable data.

Several interviews have been conducted in IT service department for Innovative technology of Coventry, which was in charge of the M-Commerce application in Coventry University and as the supplier's perspective.

According to the interview, Mr. C explained that Coventry University had thought of applying M-Commerce few months back, but dropped the idea finally. This was because first, the University was shortage of M-Commerce experience, second, IT services had insufficient knowledge, and third, there were not much research done in such an area. In addition, the university won't have any plans to implement the M-commerce in near future.

When asked why the University considered the M-Commerce, Mr. C stated that if the University could apply M-Commerce in their system, then students would be able to get benefits like accessing CU online, using e-library, checking their lecture and exam timetables, and etc. Mr. C also discussed about the factors which affect the University's decision for M-Commerce such as cost and technology. He described that implementing new technology would be more expensive. It was not wise to suggest for the application of M-Commerce in the University, where not many students have mobile phones that support WAP (Wireless Application Protocol). As other members of IT services were interviewed, they raised issues such as M-Commerce is a bit expensive than on PCs or wired cables. Hence, the University doesn't want to pay more. For example, WAP technology that works on packet system will cost more.

As a conclusion, the IT staffs added that even with lots of efforts and considering all factors for implementation, Coventry University is not ready yet to adopt M-Commerce, as they are not sure about how to make security for M-Commerce. They mentioned that with the involvement of banks in between (the University and the students), the University would take higher risks since they were not able to provide the security of M-Commerce, which both the University and the students required.

4. THE CONSUMERS' PERSPECTIVES

In order to know if the students are willing to use and ready for M-Commerce in the University, and if there are sufficient students that have latest Mobile phones for M-Commerce usage, a survey has been conducted in Coventry University in June 2009. A questionnaire has been designed based on the M-Commerce application in the University. 100 questionnaires have been sent out, and there were 80 replies. Therefore, the opinions of these repliers represent the consumers' perspectives of M-Commerce usage in the University.

The repliers are from current undergraduates and postgraduates Coventry University students, in which there are 43 males (53.8%) and 37 females (46.2%). 28.8% of the repliers are home students and 71.2% are overseas students. 70% of the surveyed students are between 21-25 years old, 8.8% are less than 20, and 21.2% are between 26-30 years old. Surprisely, over 61.2% replies have Smart phones or PDA mobile phones that can be used for M-Commerce and the rest (38.8%) have cell phones. This is against Mr. C's claim that not many students have mobile phones supporting WAP.

The Figure 1 illustrates the various mobile brands that surveyed students used, in which Orange, Vodafone, and O2 rank top three. Actually, most of the big mobile phone brands are supported by the telecom giants. For example, O2 is run and operated by British telecom; Orange WAP services is run and operated by Orange telecommunication plc.; Pan-European wireless telecommunications operator is owned by T-mobile; and Vizzavi is owned by Vodafone, a world class wireless telecommunications operator (Elliot, 2004).

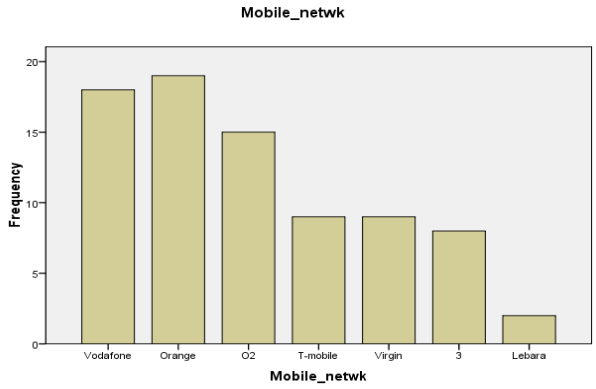

Figure 1

For the additional charge of the University M-Commerce, 77.5% of the repliers prefer free of charge, 15% of them are willing to pay 1-9 pounds per month, and only 7.5% of sample students are ready to pay 10-19 pounds.

The interesting results come from the evaluation of the preferable features of University M-Commerce. Exam date information, lecture changes and timetables, and access emails, modules and coursework are the most preferable M-Commerce applications by the sample students. However, e-journal, the University news, and paying library fines are the most disliked applications.

When asking the students to use 1-100 per cent to describe the security concerns related to the use of University M-Commerce, 13.8% of the sample students chose 85%, and both 12.5% groups weight respectively 90% and 80% for the security concerns.

In the evaluation of the reasons leading to unsuccessful M-Commerce, the top five reasons are price sensitivity, the speed of network, exposure to fraud, security/encryption, and lost of the device with valuable information. Although security is vital for the M-Commerce usage, it is sacrificed compared with the low price by the students.

For the wireless security system provided by the University, the students expressed the importance from top-down as Guaranteeing identity, Authenticity, and Confidentiality.

5. M-COMMERCE SECURITY

As the student survey shown, security is the vital concern that impedes the students using M-Commerce in the campus. This section lists the common security concerns in M-Commerce, followed by the description and evaluation of current security technologies adopted in M-Commerce. Based on the evaluation, suggestions on how to deploy trustworthy M-Commerce services are provided.

5.1 Security concerns in M-Commerce

M-Commerce shares most of the security challenges with E-Commerce. These are listed as follows:

- Authentication: the customers (the staff/students) and the service providers should be able to verity that the business partners are who they claim to be.
- Non-repudiation: the customers should be unable to deny that they have used a service or participated in a transaction. There should be an assurance that the agreements are legally binding.
- Confidentiality: Only the business partners should be able to understand the information sent/received during a transaction.
- Integrity of data: The information sent over the transaction should not be tampered with on its journey.

(Ding, 2002).

In addition, M-Commerce introduces some other security concerns, for example:

- Mobile devices are small so that they may get lost/stolen, which leads to the private information in them getting lost;
- The limited processing power and memory on mobile devices add constraints on the deployable security mechanisms;
- Platforms or applications lacking access control open doors to malicious code, which causes the confidential information on the mobile devices to get exposed.

5.2 Security technologies in M-Commerce

To gain the trust and satisfaction from M-Commerce customers, recent years have witnessed several security technologies developed and deployed by industry players. Due to space limitations, four security technologies are discussed (Ding et al 2002).

1) Secure Socket Layer (SSL)

SSL technology was developed by Netscape Communications Corporation to provide end-to-end security and privacy for communications over Internet. The SSL protocol maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes. Many leading financial institutions, such as Visa, MasterCard, American Express, etc. have endorsed SSL for commerce over the Internet.

2) Wireless Public Key Infrastructure (PKI)

PKI is a set of processes and technologies that use public key cryptography and key certification practices to secure Internet services. PKI meets the needs for securing (wireless) E-Commerce by guaranteeing authenticity, data integrity, confidentiality and non-repudiation. PKI used for the security of e-commerce in wired Internet is not suitable for the mobile phone because of the fundamental

limitation of performance such as less memory and less powerful CPU (Lee et al. 2007). Wireless PKI technology, launched by the Radicchio Initiative, is to provide the similar security level as the wired PKI while supporting mobile commerce.

3) Wireless Application Protocol (WAP) and Wireless Transport Layer Security (WTLS)

WAP technology, developed by WAP forum industry association, is an application layer standard to enable wireless access to mobile webs from a mobile phone or a PDA. WTLS is the end-to-end transport layer security protocol specific for WAP. It provides the upper layer of the WAP with privacy, data integrity and authentication between two communication applications.

4) Wired Equivalent Privacy (WEP)

WEP technology is a security protocol which aims to provide the same level of security as wired local area network on 802.11 standards. Its primary objectives are to provide confidentiality and data integrity by using a secret key shared between the communicators, and to protect access to the network infrastructure by rejecting non-WEP packets. WEP resides on the two lowest layers of the open system interconnection (OSI) model – the physical layer and the data link layer, so it does not offer end-to-end security.

In order to evaluate these technologies, Table 1 to Table 4 list the strength and weakness of these four security technologies respectively.

Table 1: Evaluation of SSL

Strength	Weakness
• Supports a secure connection between server and client; • Provides closed end-to-end security with the GSM phones; • Most widely used Internet security protocol.	• Does not provide security for individual messages; • Re-negotiation of Session Keys.

(Based on: NTRG & Ding, 2002)

Table 2: Evaluation of PKI

Strength	Weakness
• A comprehensive security system that includes two encryption keys, a digital signature, and a security certificate; • Meets the needs for securing wireless by guaranteeing identity, authenticity, confidentiality and non-repudiation.	• Not much widely used by companies; • Not fully utilised because of the poor computing power and small battery capacity of a mobile phone; • Cost and registration process.

(Based on: Search Security & Ding, 2002)

Table 3: Evaluation of WTLS

Strength	Weakness
• Provides a secure end-to-end connection for the WAP; • Provides privacy and reliability for client-server communications over a network; • Supports key refresh and transaction recovery.	• Does not cover all security features (e.g. digital signature); • Limited prevention against denial of service attacks; • Does not stop traffic analysis; • Secures data specific to a session only; • Secure sessions cannot share exchanged secrets.

(Based on: ECE & Ding, 2002)

Table 4: Evaluation of WEP

Strength	Weakness
• Provides confidentiality and data integrity, and protects access to the network infrastructure by rejecting all non-WEP packets; • Provides a good starting point for security of a WLAN.	• Easy for hackers to connect to the network; • Network Performance is degraded by up to 30%; • Static key based.

(Based on: Sam Wells, 2002 & Ding, 2002)

Further, a matrix table has been designed to compare these four technologies. As shown in Table 5, five criteria have been chosen: comprehensiveness, adoption, trust, technology reliability, and data protection. The companies that have adopted these technologies are also given. To evaluate, grades are assigned to each criterion by the authors, and the explanation why a certain number is given has been discussed as follows.

Table 5: Security technology evaluation matrix

Criteria / Grades (1-5) / Technology	Comprehensiveness	Adoption	Trust	Technology Reliability	Data protection	Companies Adopted
SSL	**3**	**3**	**3**	**2**	**3**	Nokia, Visa, Nordea, Amazon, EBay.
Wireless PKI	**4**	**2**	**4**	**3**	**3**	Microsoft, Sun Microsystems, Johnson & Johnson, And Govt. Of different

						countries.
WAP and WTLS	**3**	**3**	**2**	**3**	**2**	Google, YouTube, BBC News.
WEP	**2**	**2**	**2**	**2**	**1**	Burton Group, Core Competence Inc.

PKI is the most comprehensive (grade 4) and trusted (grade 4) security technologies but is not widely used (grade 2) due to its complexity and cost. SSL and WTLS have been adopted widely (grade 3) due to the popularity of Web and WAP. In terms of the technology reliability, SSL v2 (grade 2) contained a number of security flaws, which led to the design of SSL v3 (Rescorla 2001) which was later superseded by Transport Layer Security (TLS), an Internet Engineering Task Force (IETF) standard protocol. WTLS, derived from TLS, truncated some cryptographic elements, such as HMAC (Hash Message Authentication Code) message digests, in order to reduce transmission overhead, which potentially reduced the data integrity protection (grade 2). WEP alone, due to its original design purpose, can not provide end to end security, and therefore, the lower grade 2 is given in the first four criteria, but grade 1 is given in Data protection.

6 Conclusion

So far no end-to-end security technology claims that it can address all security concerns for M-Commerce. However, these security technologies and frameworks are continuously evolving. Existing security technologies, such as WTLS and wireless PKI, or SSL and PKI, can be joined to provide more powerful security. Furthermore, new security technologies are emerging such as quantum cryptography that is able to detect eavesdropping and guarantees key security.

According to the survey, over 60% of the students have a mobile phone available for M-Commerce, and most of the surveyed students showed the interests of the campus M-Commerce, which means students are more ready for the campus M-Commerce than the University expected. However, over 70% of the students prefer to use campus M-Commerce for free, although about 20% of them are willing to pay less than 20 pounds per month. Message of exam dates, notification of lecture changes & timetable, and access to emails, modules and coursework rank the top three most preferable demands of campus M-Commerce.

Therefore, it is suggested that the university start the M-Commerce without any charge by providing those services that don't require high level of security, such as accessing emails, modules and coursework service, or notification of lecture changes, timetable, and exam date service. Then it can be followed by the upgrade level of M-Commerce such as paying fines or car parking fees.

It should be noted that the technologies alone cannot solve the security in M-Commerce. Lawmakers, regulatory bodies and the technology providers should work together towards providing end-to-end secure wireless communications for M-Commerce. If so, users' confidence on M-Commerce will be built up soon, and more and more students/staff will be using M-Commerce services if the university provides them.

References

1. W. C. Hu, C. W. Lee, et al. (2004), Mobile Commerce Applications, in N. S. Shi (ed.), Mobile Commerce Systems, Idea Group Publishing.

2. C. W. Lee, W. Kou, and W. Hu (2004), Mobile commerce security and payment methods. Hershey, PA, USA: Idea group publishing

3. T. T. Wei, G. Marthandan, et al. (2009), "What drives Malaysian m-commerce adoption? An empirical analysis", *Industrial Management & Data Systems*, vol. 109, no. 3, pp. 370-388

4. D. Kao, and J. Decou (2003), "A strategy- based model for e-commerce planning", *theoretical with application in practice,* vol. 103, no. 4, pp. 238-252

5. G. Elliott and N. Phillips (2004), Mobile commerce & wireless computing systems, Pearson Education

6. T. P. Liang, C. W. Huang, et al. (2007), "Adoption of mobile technology in business: a fit - viability model", *Industrial Management & Data Systems,* vol. 107, no. 8, pp. 1154-1169.

7. L. D. Chen, and G. Skelton (2005), Mobile Commerce Application Development, CyberTech Publishing.

8. S. Deibert, and F. Rothlauf (2006), On the Benefit of Using Mobile Technologies in Business Processes, [online] http://wifo1.bwl.uni-mannheim.de/fileadmin/files/publications/Working_Paper_eChallenges06.pdf [Access date: 9 March, 2009]

9. A. Segev (2003), Assessing the Business Value of Mobile Applications1, [online] http://www.research.att.com/~rjana/Segev.pdf [Accessed date: 12 March, 2009]

10. M. Khalifa, and K. N. Shen (2008), "Explaining the adoption of transactional B2C mobile commerce", *Journal of Enterprise Information Management,* vol. 21, no. 2, pp. 110-124.

11. D. V. Thanh, (2003), Advances in Mobile Commerce Technologies, in E. P. Lim and K. Siau (ed.), Mobile E-Commerce on Mobile Phones, Idea Group Inc.

12. Qpass (2004), Consumer Study Spotlights Unmet M-Commerce Opportunity for Mobile Operators, [online] http://www.mobileeurope.co.uk/news_wire/11867/Consumer_Study_Spotlights_Unmet_M-Commerce_Opportunity_for_Mobile_Operators.html [Accessed date: 9 May, 2009]

13. S. Barnes (2007), E-commerce and v-business, Elsevier

14. S. Barnes (2007), E-commerce and v-business: digital enterprise in the twenty-first century, Elsevier.
15. VeriSign. (2007), Mobile Commerce Services - Driving Mobile Commerce Adoption: Best Practices for a Comprehensive, Secure Mobile Commerce Strategy, [online] http://whitepapers.techrepublic.com.com/abstract.aspx?docid=285557 [Accessed date: 14 May, 2009]
16. R. Tiwari, S. Buse, et al. (2008), From Electronic to Mobile Commerce: Opportunities through technology convergence for business services, [online] http://www.cacci.org.tw/Journal/2008%20Vol%201/FromElectronic.pdf [Accessed date: 17 May, 2009]
17. P. Davidson (2006), Ad campaigns for your tiny cellphone screen get bigger, USA TODAY, 8 Sept. 2006. [online] http://www.usatoday.com/tech/wireless/2006-08-08-mobile-ads_x.htm [Accessed date: 29 June, 2009]
18. G. Armstrong, and P. Kotler (2009), Marketing- in introduction, 9th edition, Pearson
19. Portio Research (2008), Mobile Messaging Futures 2009-2013 - Analysis and Growth Forecasts for Mobile Messaging Markets Worldwide: 3rd Edition, [online] http://www.portioresearch.com/ [Accessed date: 23 June, 2009]
20. Mobile Marketing Magazine, 25 Sept. 2008, 80% of World's Population on Mobile by 2013, Says Portio, [online] http://www.mobilemarketingmagazine.co.uk/2008/09/80-of-worlds-po.html [Accessed date: 23 June, 2009]
19. Mobile Marketing Magazine, 13 Nov. 2008, Sponge Reveals Mobile Microsite Research Findings, [online] http://www.mobilemarketingmagazine.co.uk/2008/11/sponge-reveals.html [Accessed date: 23 June, 2009]
20. R. Tiwari, S. Buse and C. Herstatt (2008), "From Electronic to Mobile Commerce", *CACCI Journal*, vol. 1, 2008
21. D. Taniar, Editor (2008), Mobile computing: concepts methodologies, tools and applications, Information Science Reference
22. M. S. Ding, and C. R. Unnithan (2002), Mobile Commerce (mCommerce) Security: An Appraisal of Current Issues and Trends, [online] http://www.deakin.edu.au/infosys/research/working_paper.htm [Accessed date: 23 June, 2009]
23. Y. Lee, J. Lee, and J. Song (2007), "Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce Source", *Computer Communications,* vol. 30, no. 4, pp. 893-903
24. E. Rescorla, (2001), SSL and TLS: Designing and Building Secure Systems, United States: Addison-Wesley
25. S. Wells (n. d.), 802.11 WLAN Security — Choose Wisely! [online] http://www.bechtel.com/communications/assets/files/TechnicalJournals/December2002/Article11.pdf [Accessed date: 22 June, 2009]
26. NTRG (Networks and Telecommunications research Group) (n. d.) Weakness Of SSL Protocol [online] http://ntrg.cs.tcd.ie/mepeirce/Dce/99/ssl/weak.htm [Accessed date: 21 June, 2009]
27. M. Cobb (n. d.), Search Security [online] http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1217799,00.html [Accessed date: 23 June, 2009]
28. Mishra (n. d.), Strength and weakness of WTLS [online] http://www.ece.mtu.edu/ee/faculty/mishra/Presentations/IPSECvsWTLS.pdf [Accessed date: 20 June, 2009]